REMARKS/ARGUMENTS

Applicants have now had an opportunity to carefully consider the Examiner's comments set forth in the Non-Final Office Action of May 19, 2005. Reconsideration of the Application is respectfully requested.

The Office Action

Claims 1, 4, 5 and 6 were rejected under 35 USC 103(a) as being unpatentable over Haber (US Pat. No. 5,136,647) in view of Romney (US Pat. No. 6,038,322) in further view of Berson (US Pat. No. 5,949,879). Claim 3 was rejected under 35 USC 103(a) as being unpatentable over Haber, Romney and Berson as applied to claim 1 and in further view of Lirov (US Pat. No. 6,785,810). Claim 7 was rejected under 35 USC 103(a) as being unpatentable over Haber, Romney and Berson as applied to claim 1 and in further view of Doyle (US Pat. No. 6,381,696).

Status of the Claims

Claims 1, 3, and 5-16 are pending in this application. Claims 2 and 4 have been canceled. Claims 8-16 have been added. Support for the new claims may be found throughout the specification, and, more particularly, on page 6, lines 12-15 (claim 8), on page 7, lines 2-5 (claim 9), on page 7, lines 11-13 (claim 10), and on pages 5-7 (claims 11-16).

The Pending Claims Are Patentable Under 35 USC 103(a)

The present application teaches an improved method for securing the integrity of files prior to archiving and involves an exchange between a client and a Time Source Provider. Claim 1, as amended, provides, among other things, that both the Client and the Time Source Provider must have the ability to generate Public and Private Key pairs, that the client's Public and Private Key pair is associated with an organization, a corporate unit or an individual, that the Client encrypts the data with the Client's Private Key and then with the Public Key of the Time Source Provider, that the encrypted data and file attributes along with the client's Public Key are to be transmitted to the Time Source Provider, and that the Time Source Provider decrypts the encrypted data and file attributes with the Time Source Provider's Private Key and with the client's Public Key. Thus, if the key pair is

reserved for archiving, then the risk of exposure and compromising is decreased. None of these concepts are fairly taught or suggested by the references cited by the Examiner.

Haber relates generally to a method of time-stamping a digital document and authenticating the document by means of the agency's public key to reveal the receipt. The receipt comprises the hash of the alleged document along with the time seal that only the agency could have signed into the certificate. However, Haber does not teach or suggest, for example, the steps of generating Private and Public Key pairs for the client and the Time Source Provider using the Key pairs for encrypting and decrypting the data and file attributes.

While Romney arguably discloses the step of the client generating a public/private key pair (see FIG. 2), Romney does not disclose the additional steps of the Time Source Provider generating *its own public/private key pair*, whereby the two sets of key pairs are used to encrypt and decrypt the data and file attributes.

The newly cited reference, Berson, provides for an auditable, secure environment for the generation of cryptographically protected digital data. However, Berson does not teach associating the client's Public and Private Key pair with an organization, a corporate unit or an individual. In column 4, lines 29-34, of Berson, there is a reference to the generation of a unique client master cryptographic key pair, which includes an encryption key and a decryption key. However, there is no discussion of having different key pairs for certain groups or individuals within the corporate structure of the client. Rather, the reference in Berson to the key pair and to a "certificate" is more along the lines of what is mentioned in the specification as being an option. That is, "the keys exchanged between the client and the Time Source Provider could be embedded in any number of digital certificates thereby allowing for secure future checks from an independent Certificate Authority." (See page 9, lines 14-18, of the specification.) This is distinguishable from the concept of "organizationally associating" the client's key pair.

Likewise, Berson fails to teach or suggest encrypting the files with the client's private key and the Time Source Provider's public key and decrypting the files with the Time Source Provider's private key and the client's public key.

Accordingly, claim 1 and the claims depending therefrom (3 and 5-10) are not obvious in view of the cited references.

Claim 5 is further patentable in that it includes the limitation of applying multiple or

differing error correcting codes to the representation of the time, the time source calibration data, the file attributes and encryption key signatures. Although Berson does refer to a routine for determining communication errors, it does not teach or suggest "multiple or differing error correcting codes," let alone specific codes for (a) time, (b) time source calibration data, (c) file attributes, or (d) encryption key signatures. As such claim 5 (and claim 16) is patentably distinguishable.

Claim 6, as amended, is further patentable in that it includes the steps of the client producing the archived files, file attributes and time map, the Time Source Provider retrieving the time map and session key, the Time Source Provider regenerating the time map, the Time Source Provider encrypting the time map with the session key, and comparing the regenerated time map to the time map. Thus, claim 6 relates to a request for legal verification of authenticity and/or the time of archival of files, whereby the client would only have to produce the archive file and any encryption keys used by the client. (See page 8, lines 1-3, of the present application.) The originality of the time and time map may be readily verified by the method of claim 6. (See page 8, lines 6-8, of the present application.)

Haber fails to disclose the additional features of claim 6. As such, the Examiner claims that Romney teaches the method of claim 6. As disclosed in col. 7, lines 34-37, of Romney, the electronic document and the public/private key pair may be sent to the authenticator by electronic means. As noted in col. 7, lines 42-47, the authenticator may, for example, take biometric readings of the client for identification. However, there is no mention of a "session key," as provided in claim 6.

New claims 11-16 are not obvious in view of the cited references.

CONCLUSION

For the reasons detailed above, it is submitted that all claims remaining in the application (Claims 1, 3 and 5-16) are now in condition for allowance. The foregoing comments do not require unnecessary additional search or examination.

No additional fee is believed to be required for this Amendment. However, the undersigned attorney of record hereby authorizes the charging of any necessary fees, other than the issue fee, to Xerox Deposit Account No. 24-0037.

In the event the Examiner considers personal contact advantageous to the

disposition of this case, he/she is hereby authorized to call John S. Zanghi, at Telephone Number (216) 861-5582.

Respectfully submitted,

FAY, SHARPE, FAGAN,
MINNICH & McKEE, LLP

8/19/05
Date

John S. Zanghi
Reg. No. 48,843
1100 Superior Avenue, 7th Floor
Cleveland, Ohio 44114-2579
(216) 861-5582

N:\XERZ\200696\EMC0002999V001.DOC